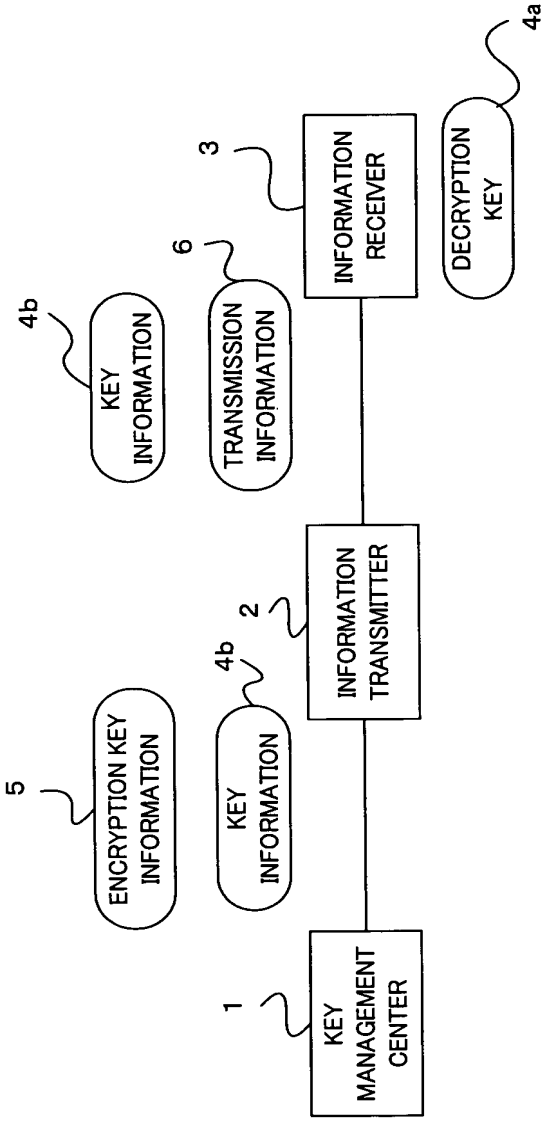

KEY MANAGEMENT CENTER
1
INFORMATION TRANSMITTER
2
INFORMATION RECEIVER
3
ENCRYPTION KEY INFORMATION
5
KEY INFORMATION
4b
TRANSMISSION INFORMATION
6
DECRYPTION KEY
4a

FIG. 1A

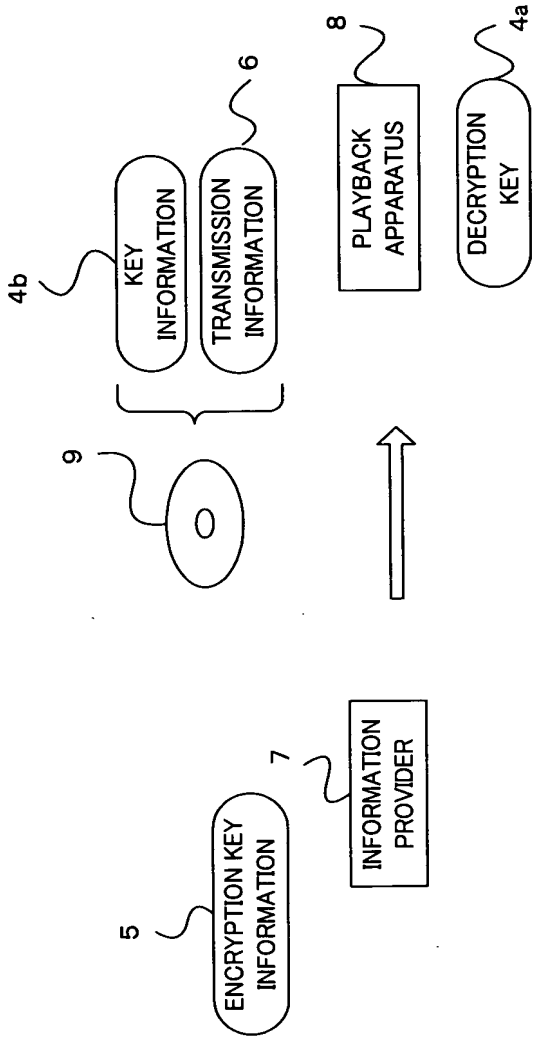

ENCRYPTION KEY INFORMATION
5
INFORMATION PROVIDER
7
KEY INFORMATION
4b
TRANSMISSION INFORMATION
6
9
PLAYBACK APPARATUS
8
DECRYPTION KEY
4a

FIG. 1B

10/527992

FIG. 2

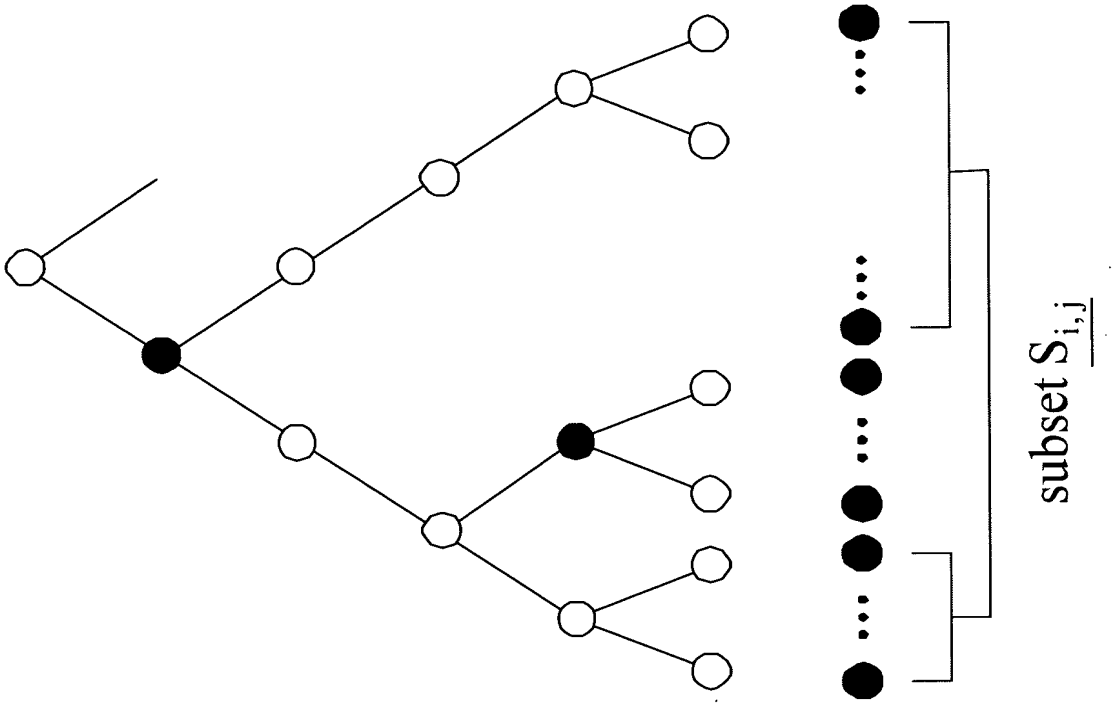


FIG. 3A

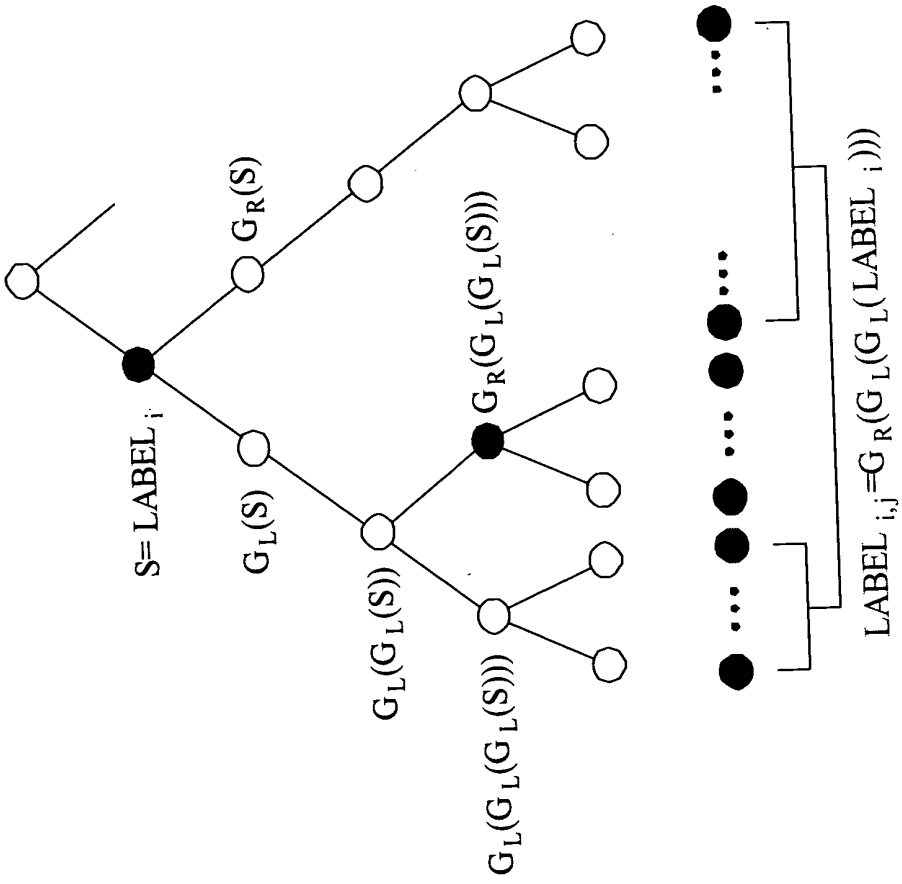

S= LABEL i
G L(S)
G R(S)
G L(G L(S))
G R(G L(S))
G L(G L(G L(S)))
LABEL i,j =G R(G L(G L(LABEL i)))
L i,j =G M(LABEL i,j)

FIG. 3B

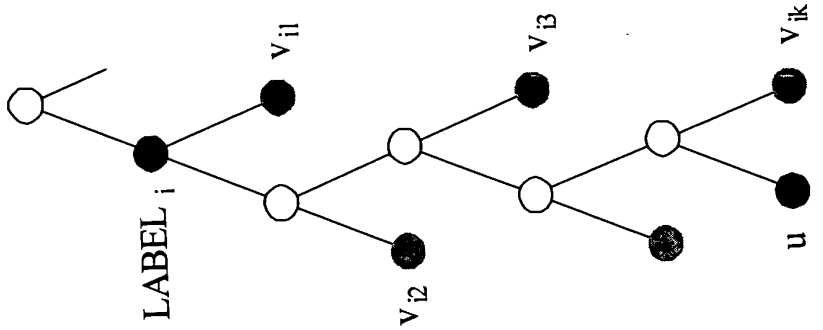

LABEL i
v i1
v i2
v i3
v ik
u

FIG. 4

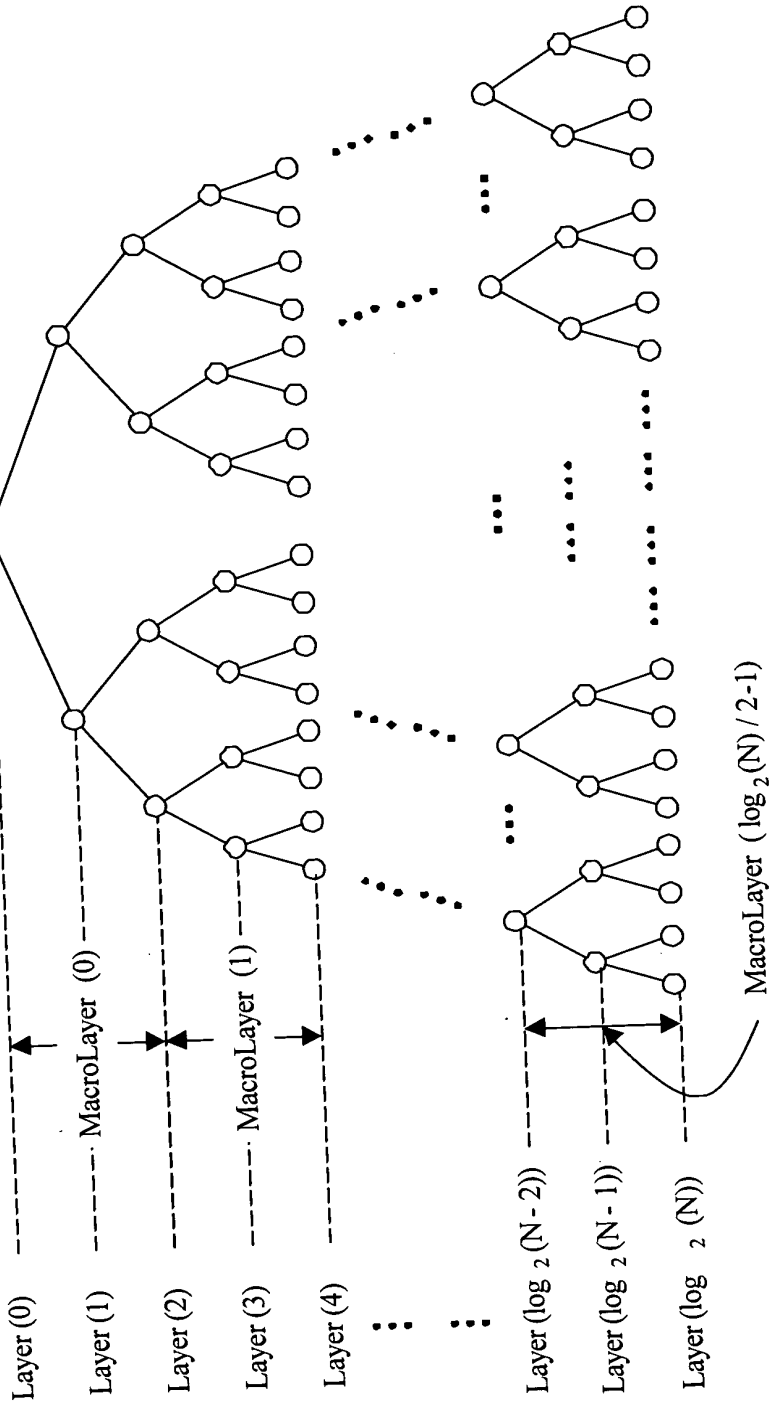

Layer (0)
Layer (1)
Layer (2)
Layer (3)
Layer (4)
Layer (log 2 (N - 2))
Layer (log 2 (N - 1))
Layer (log 2 (N))
MacroLayer (0)
MacroLayer (1)
MacroLayer (log 2 (N) / 2-1)

FIG. 5

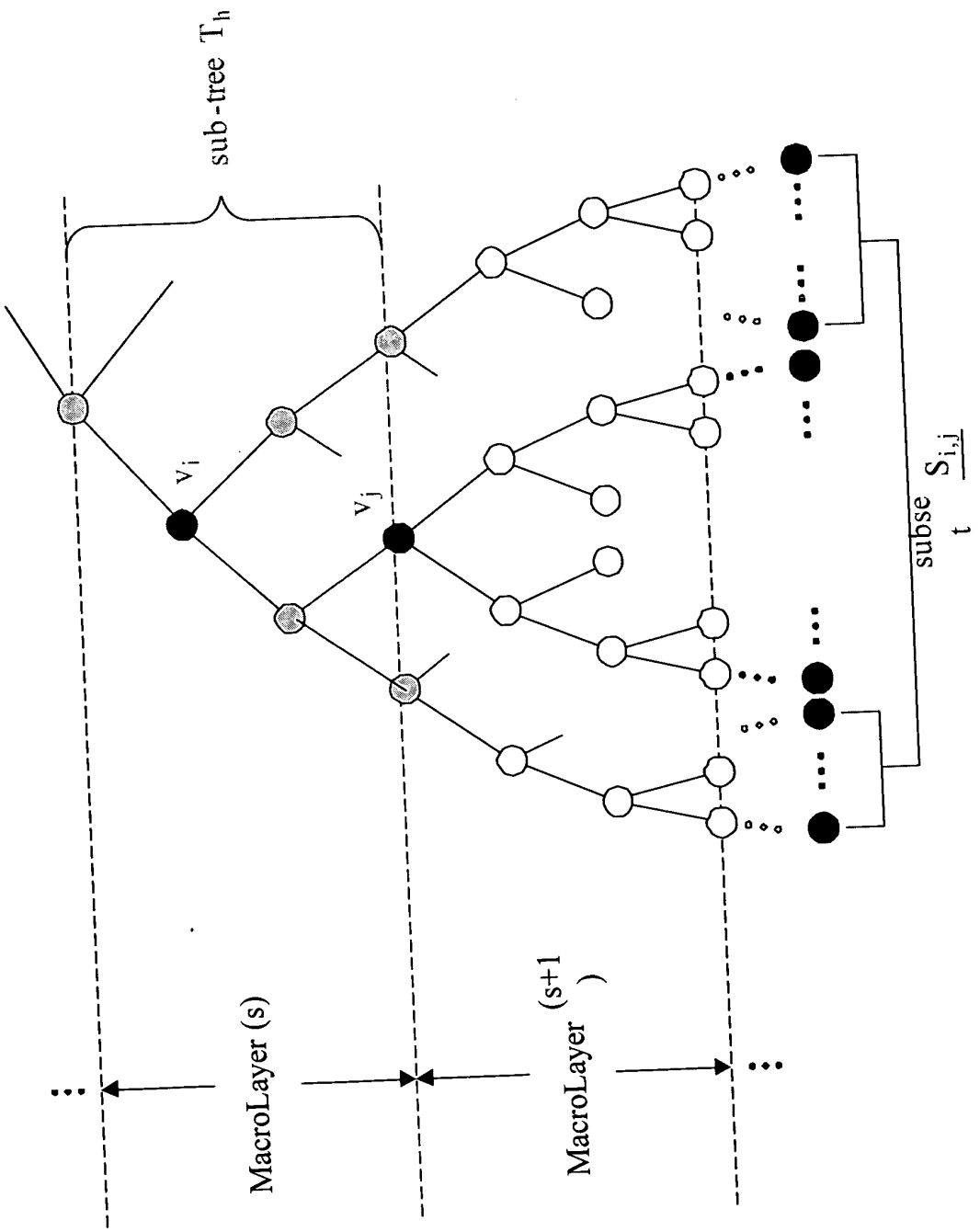


FIG. 6

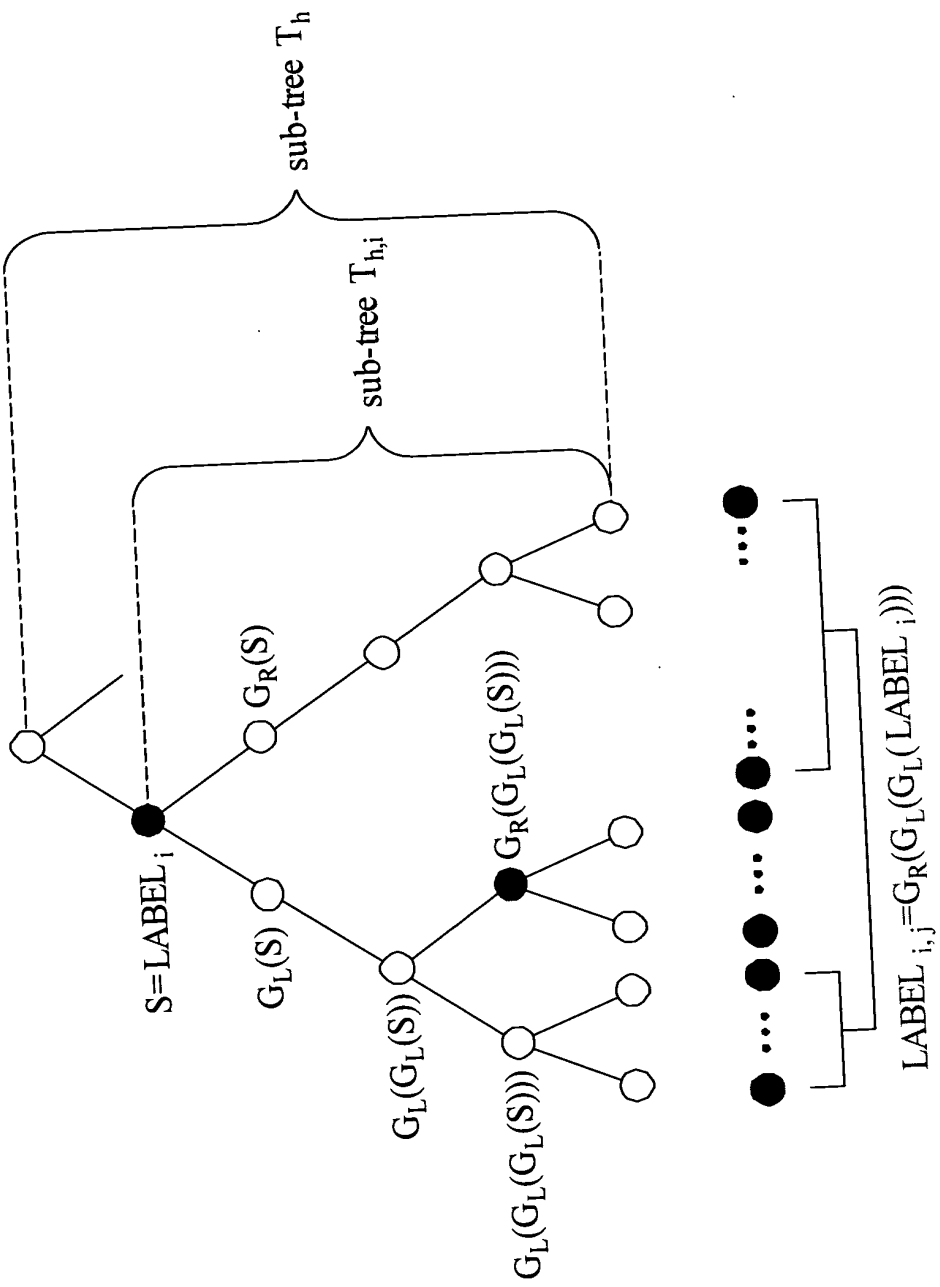

sub-tree T_h
sub-tree $T_{h,i}$
S=LABEL$_i$
$G_L(S)$
$G_R(S)$
$G_L(G_L(S))$
$G_R(G_L(G_L(S)))$
$G_L(G_L(G_L(S)))$
LABEL$_{i,j}$=$G_R(G_L(G_L($LABEL$_i$$)))$
$L_{i,j}$=$G_M($ LABEL$_{i,j}$ $)$

FIG. 7

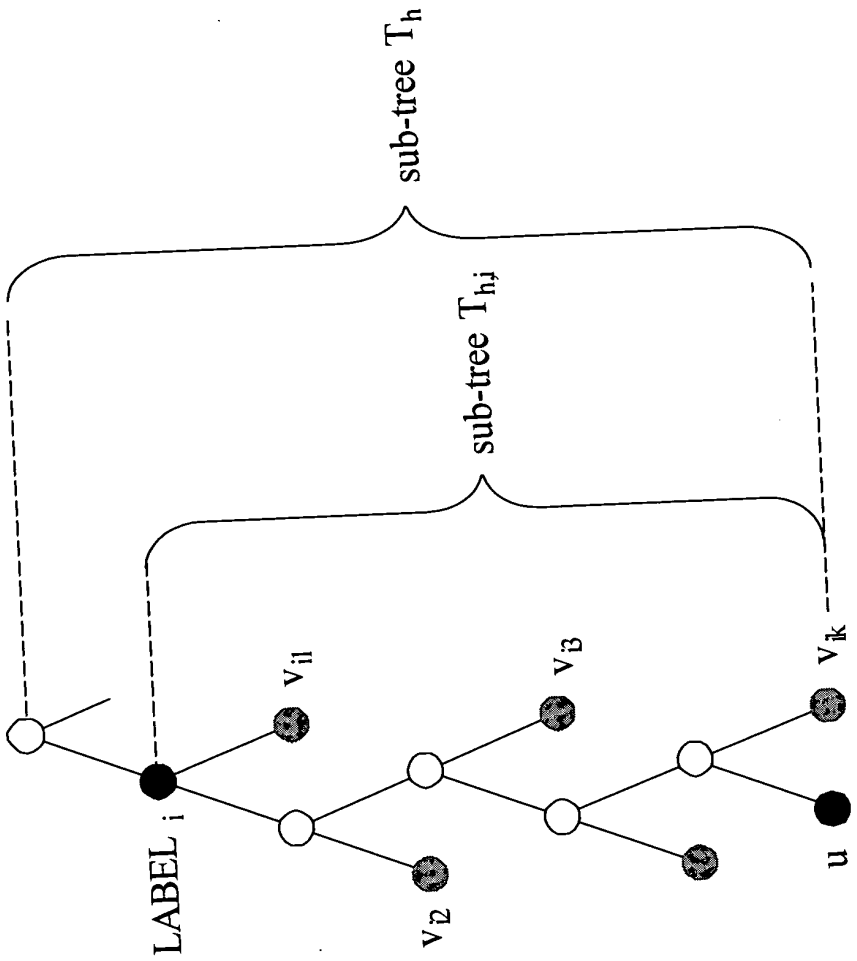


FIG. 8

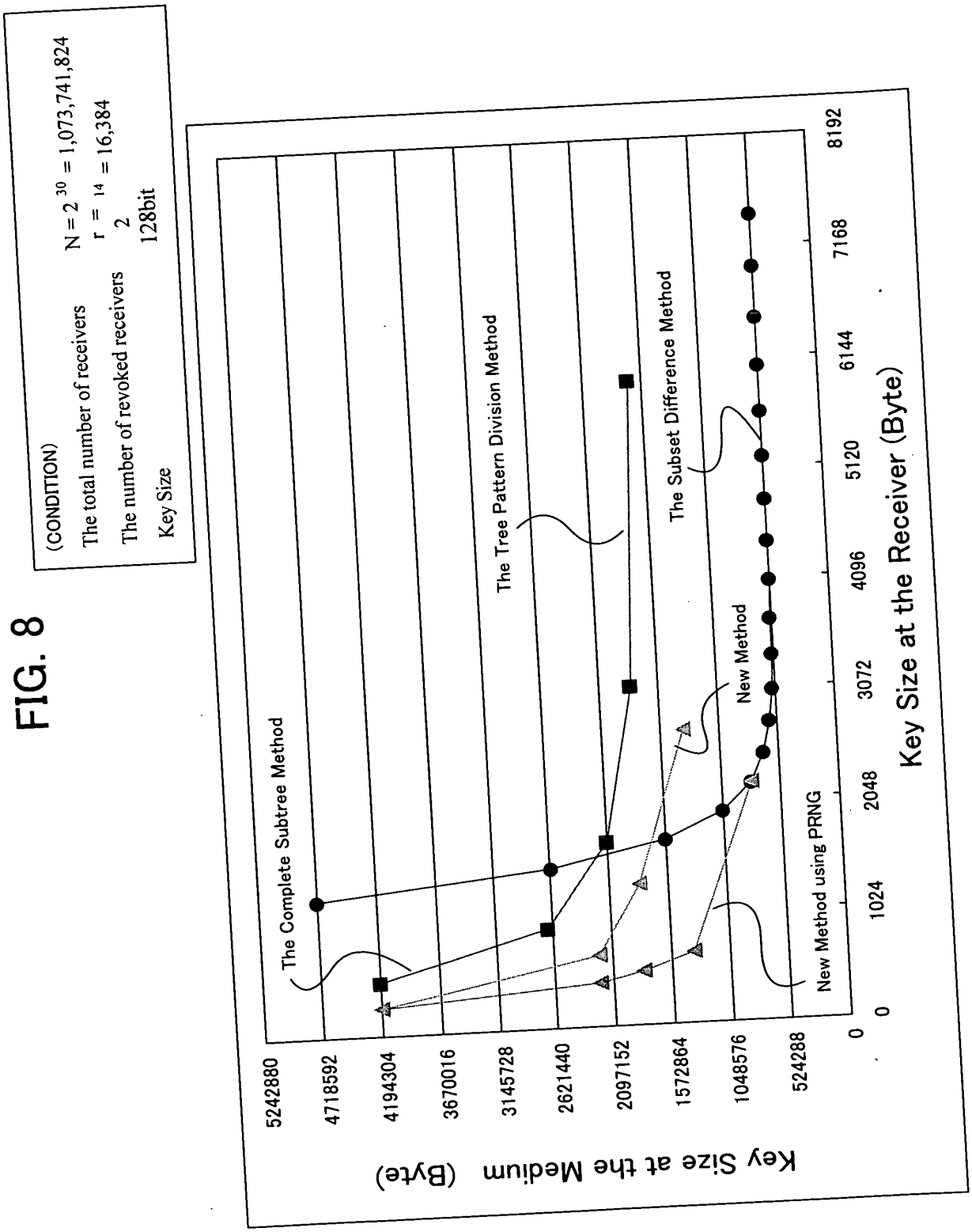
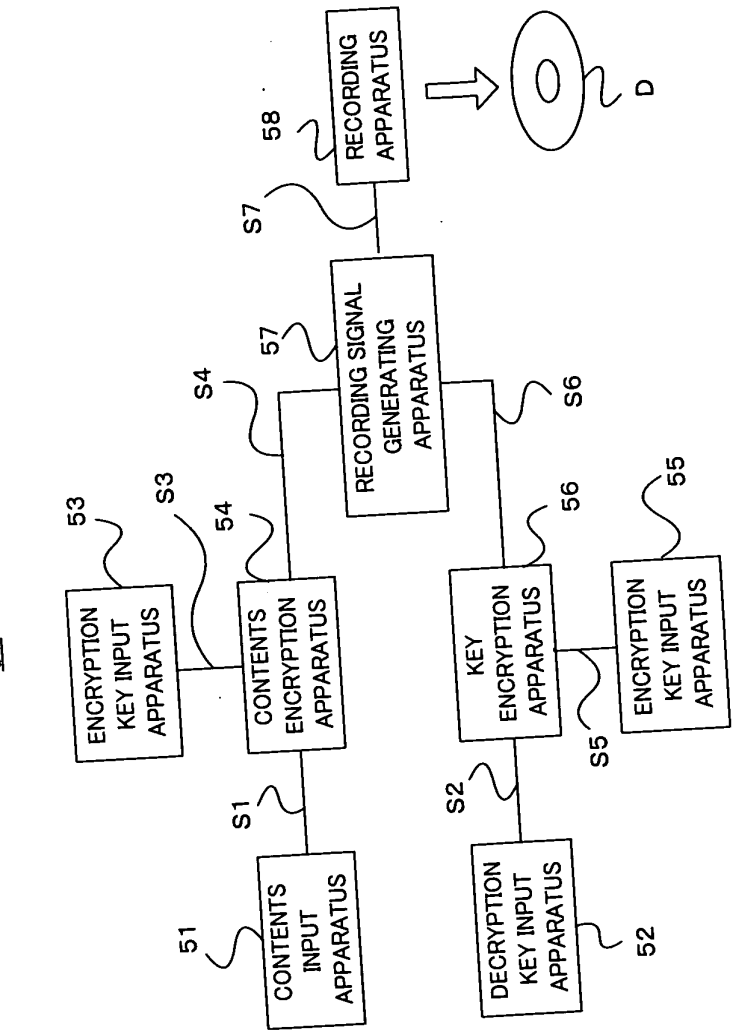

(CONDITION)
The total number of receivers N = 2 30 = 1,073,741,824
The number of revoked receivers r = 14 = 16,384
Key Size 2 128bit
Key Size at the Medium (Byte)
5242880
4718592
4194304
3670016
3145728
2621440
2097152
1572864
1048576
524288
The Complete Subtree Method
The Tree Pattern Division Method
The Subset Difference Method
New Method
New Method using PRNG
0
1024
2048
3072
4096
5120
6144
7168
8192
Key Size at the Receiver (Byte)

FIG. 9


50
CONTENTS INPUT APPARATUS
51
DECRYPTION KEY INPUT APPARATUS
52
ENCRYPTION KEY INPUT APPARATUS
53
CONTENTS ENCRYPTION APPARATUS
54
ENCRYPTION KEY INPUT APPARATUS
55
KEY ENCRYPTION APPARATUS
56
RECORDING SIGNAL GENERATING APPARATUS
57
RECORDING APPARATUS
58
S1
S2
S3
S4
S5
S6
S7
D

JC06 Rec'd PCT/PTO 21 MAR 2005

FIG. 10A SIGNAL S1

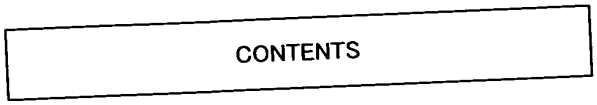


FIG. 10B SIGNAL S2

FIG. 10C SIGNAL S3

FIG. 10D SIGNAL S4

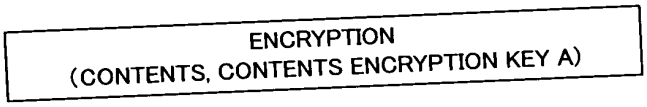


FIG. 10E SIGNAL S5

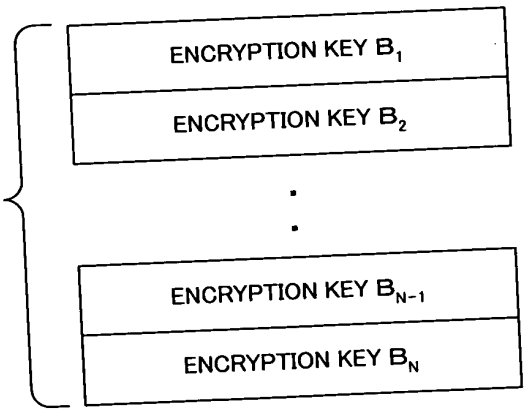


FIG. 11A

SIGNAL S6

HEADER (HEADER ENCRYPTION KEY B_1)	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_1)
HEADER (HEADER ENCRYPTION KEY B_2)	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_2)
⋮	
HEADER (HEADER ENCRYPTION KEY B_{N-1})	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_{N-1})
HEADER (HEADER ENCRYPTION KEY B_N)	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_N)

FIG. 11B

SIGNAL S7

HEADER (HEADER ENCRYPTION KEY B_1)	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_1)
HEADER (HEADER ENCRYPTION KEY B_2)	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_2)
⋮	
HEADER (HEADER ENCRYPTION KEY B_{N-1})	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_{N-1})
HEADER (HEADER ENCRYPTION KEY B_N)	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_N)
ENCRYPTION (ENCRYPTION CONTENTS, CONTENTS ENCRYPTION KEY A)	
ERROR CORRECTING CODE	

FIG. 12

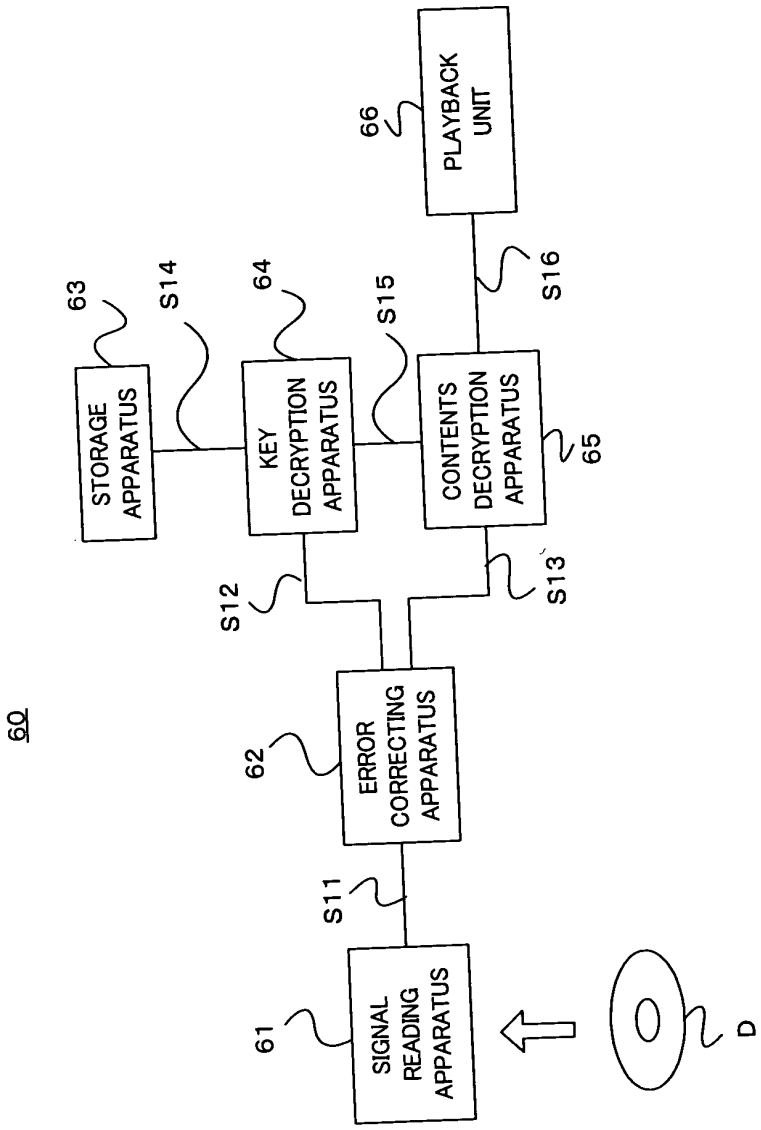

60
61
SIGNAL READING APPARATUS
62
ERROR CORRECTING APPARATUS
63
STORAGE APPARATUS
64
KEY DECRYPTION APPARATUS
65
CONTENTS DECRYPTION APPARATUS
66
PLAYBACK UNIT
S11
S12
S13
S14
S15
S16
D

FIG. 13A

SIGNAL S11

HEADER (HEADER ENCRYPTION KEY B_1)	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_1)
HEADER (HEADER ENCRYPTION KEY B_2)	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_2)
•	•
•	•
HEADER (HEADER ENCRYPTION KEY B_{N-1})	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_{N-1})
HEADER (HEADER ENCRYPTION KEY B_N)	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_N)
ENCRYPTION (ENCRYPTION CONTENTS, CONTENTS ENCRYPTION KEY A)	
ERROR CORRECTING CODE	

FIG. 13B

SIGNAL S12

HEADER (HEADER ENCRYPTION KEY B_1)	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_1)
HEADER (HEADER ENCRYPTION KEY B_2)	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_2)
•	•
•	•
HEADER (HEADER ENCRYPTION KEY B_{N-1})	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_{N-1})
HEADER (HEADER ENCRYPTION KEY B_N)	ENCRYPTION (ENCRYPTION CONTENTS DECRYPTION KEY A, ENCRYPTION KEY B_N)

10/527992

FIG. 14A

SIGNAL S13

ENCRYPTION (ENCRYPTION CONTENTS, CONTENTS ENCRYPTION KEY A)

FIG. 14B

SIGNAL S14

HEADER (HEADER DECRYPTION KEY B_1)	DECRYPTION KEY B_1
HEADER (HEADER DECRYPTION KEY B_1)	DECRYPTION KEY B_2
⋮	
HEADER (HEADER DECRYPTION KEY B_{M-1})	DECRYPTION KEY B_{M-1}
HEADER (HEADER DECRYPTION KEY B_M)	DECRYPTION KEY B_M

FIG. 14C

SIGNAL S15

CONTENTS DECRYPTION KEY A

FIG. 14D

SIGNAL S16

CONTENTS

FIG. 15

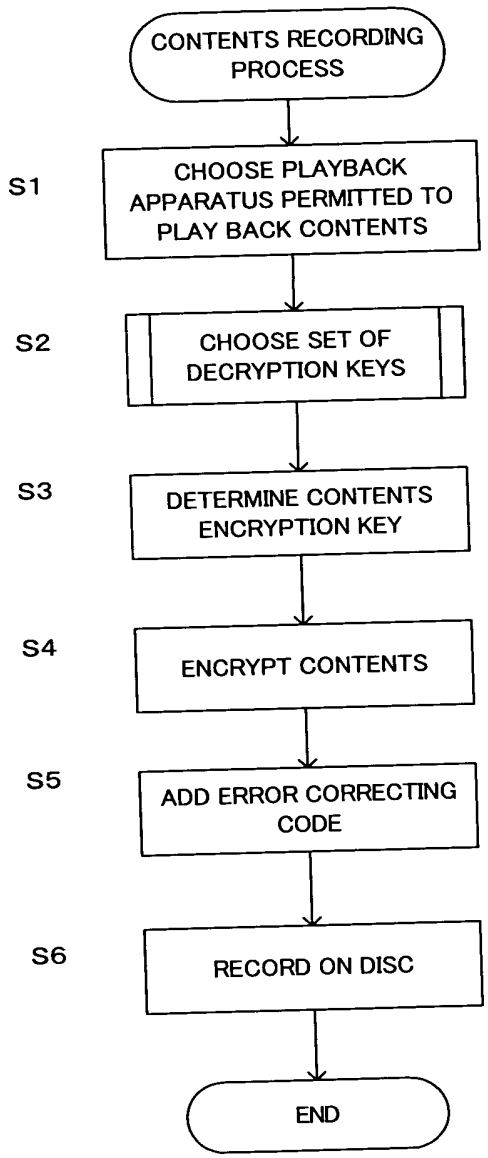

CONTENTS RECORDING PROCESS
S1
CHOOSE PLAYBACK APPARATUS PERMITTED TO PLAY BACK CONTENTS
S2
CHOOSE SET OF DECRYPTION KEYS
S3
DETERMINE CONTENTS ENCRYPTION KEY
S4
ENCRYPT CONTENTS
S5
ADD ERROR CORRECTING CODE
S6
RECORD ON DISC
END

FIG. 16

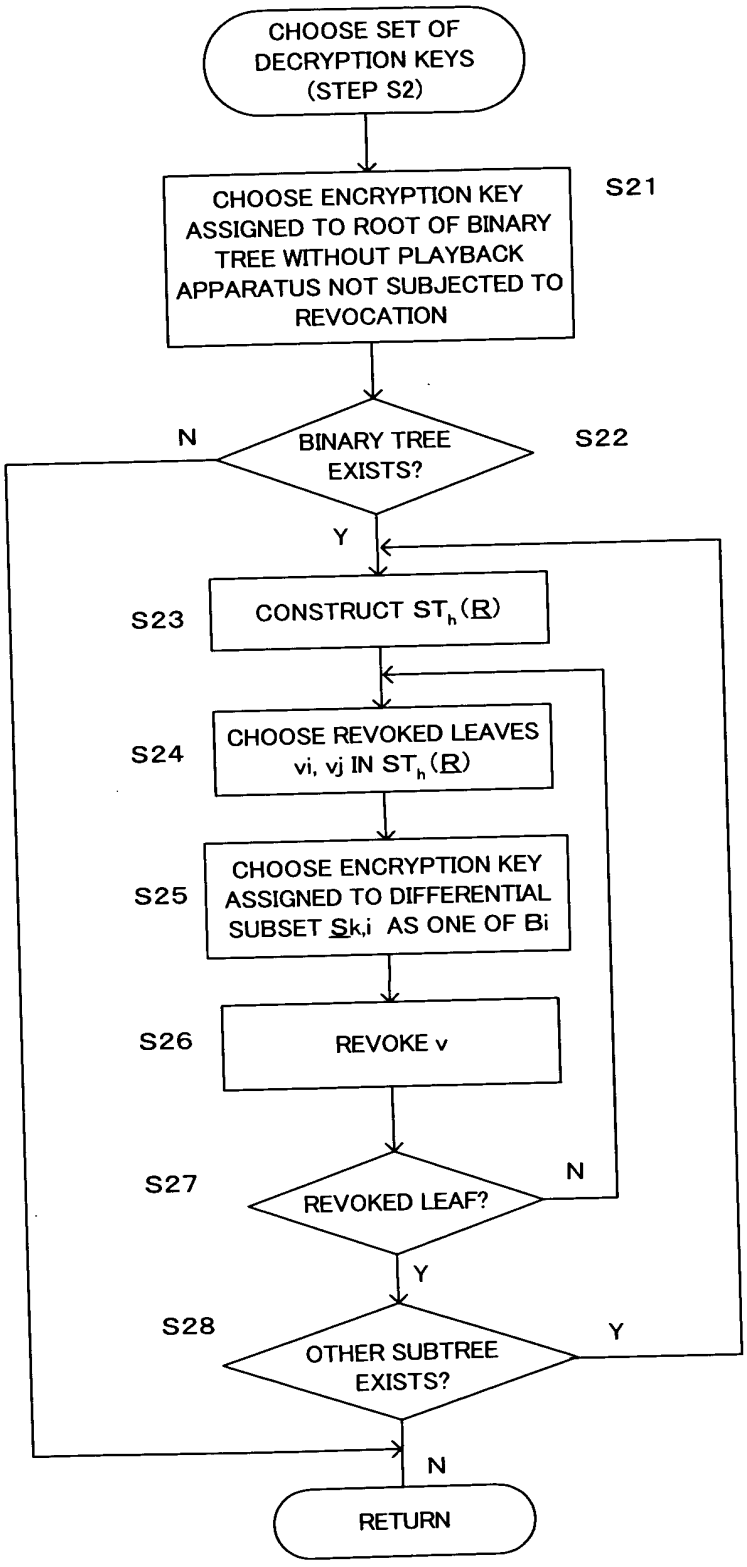
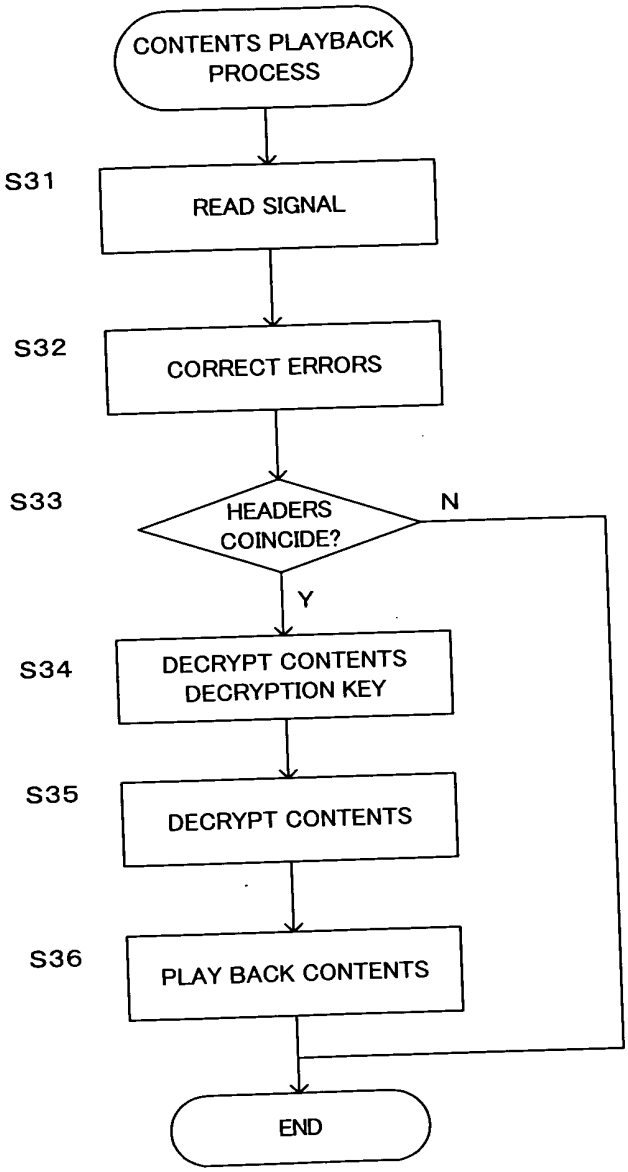

CHOOSE SET OF DECRYPTION KEYS (STEP S2)
CHOOSE ENCRYPTION KEY ASSIGNED TO ROOT OF BINARY TREE WITHOUT PLAYBACK APPARATUS NOT SUBJECTED TO REVOCATION
S21
BINARY TREE EXISTS?
S22
N
Y
CONSTRUCT ST$_h$(R)
S23
CHOOSE REVOKED LEAVES vi, vj IN ST$_h$(R)
S24
CHOOSE ENCRYPTION KEY ASSIGNED TO DIFFERENTIAL SUBSET Sk,i AS ONE OF Bi
S25
REVOKE v
S26
REVOKED LEAF?
S27
N
Y
OTHER SUBTREE EXISTS?
S28
Y
N
RETURN

FIG. 17


CONTENTS PLAYBACK PROCESS
S31
READ SIGNAL
S32
CORRECT ERRORS
S33
HEADERS COINCIDE?
N
Y
S34
DECRYPT CONTENTS DECRYPTION KEY
S35
DECRYPT CONTENTS
S36
PLAY BACK CONTENTS
END

JC09 Rec'd PCT/PTO 21 MAR 2005

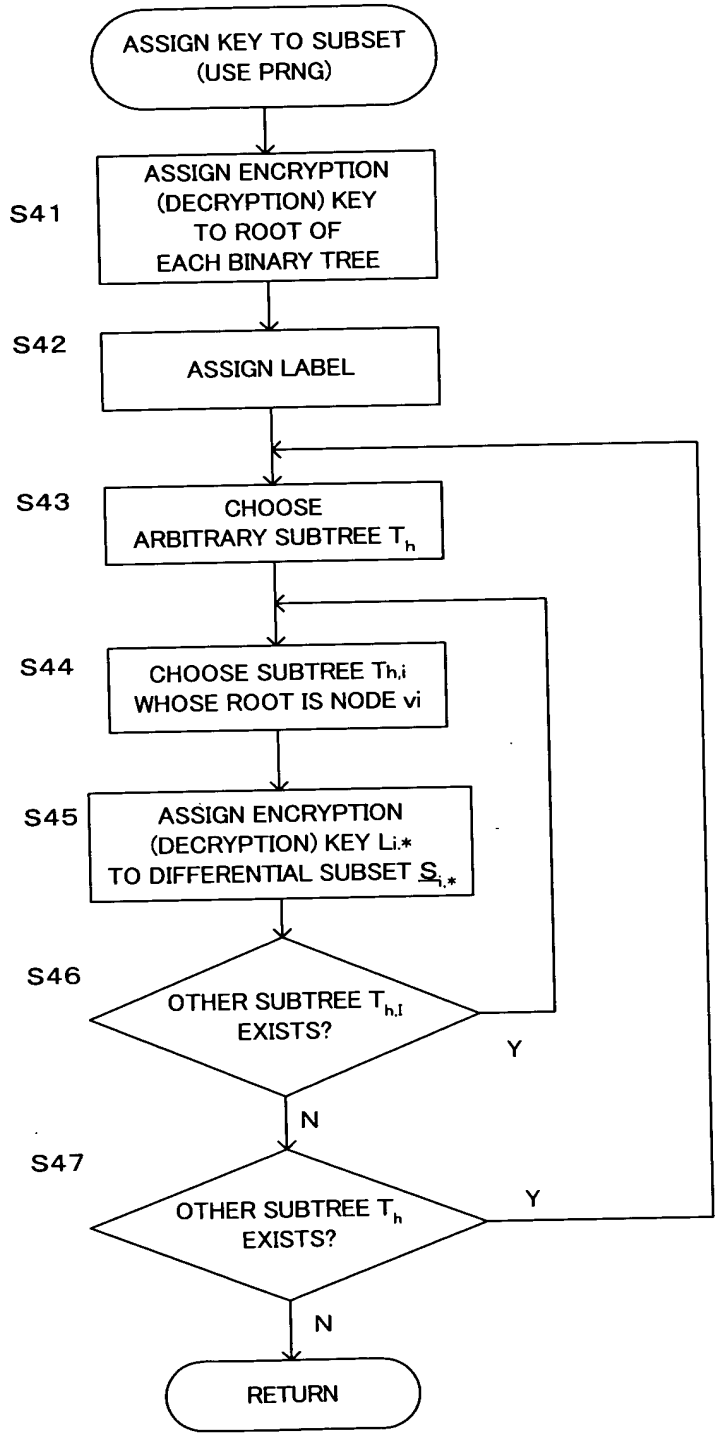



FIG. 18